

What is claimed is:

1 1. A method of achieving context-sensitive confidentiality among security domains within a
2 federated environment, the method comprising steps of:
3 determining a route to be taken by a message to be transmitted in the federated
4 environment, where the route spans a plurality of the security domains;
5 determining rights of nodes to be encountered on the determined route to access security-
6 sensitive portions of the message;
7 selectively protecting the security-sensitive portions of the message, according to the
8 determined access rights; and
9 transmitting the message with its selectively-protected portions on the determined route.

1 2. The method according to Claim 1, wherein the selectively protecting step further
2 comprises the step of encrypting at least one security-sensitive portion of the message.

1 3. The method according to Claim 1, wherein the selectively protecting step further
2 comprises the step of computing a digital signature over at least one security-sensitive portion of
3 the message.

1 4. The method according to Claim 1, wherein the step of determining the route further
2 comprises the step of consulting policy to determine the route to be taken for this message.

1 5. The method according to Claim 1, wherein the step of determining the access rights

2 further comprises the step of consulting policy for each of the nodes to be encountered.

1 6. The method according to Claim 1, further comprising the step of determining a role of at
2 least one of the nodes to be encountered, and wherein the step of determining the access rights
3 further comprises the step of consulting policy for each determined role, wherein the policy
4 specifies access rights for that role.

1 7. The method according to Claim 1, wherein the selectively protecting step further
2 comprises the step of encrypting each security-sensitive portion of the message for each node
3 determined to have access rights to that portion.

1 8. The method according to Claim 7, wherein the encrypting step uses a public key
2 associated with each of the nodes for which the encrypting step operates.

1 9. The method according to Claim 1, wherein the determined route is specified in the
2 transmitted message.

1 10. The method according to Claim 1, further comprising the step of determining a role of at
2 least one of the nodes to be encountered, and wherein the selectively protecting step further
3 comprises the step of encrypting each security-sensitive portion of the message for each of the
4 roles that are determined to have access rights to that portion.

1 11. The method according to Claim 10, wherein the encrypting step uses a public key
2 associated with each of the roles for which the encrypting step operates.

1 12. The method according to Claim 1, further comprising the steps of:
2 receiving the transmitted message at a selected one of the nodes on the determined route;
3 and
4 securely accessing only those ones of the selectively-protected portions of the received
5 message to which the selected node has access rights.

1 13. The method according to Claim 1, wherein the transmitted message contains information
2 identifying an authentication authority from a first of the security domains, and indicates that this
3 authentication authority has already authenticated a party for which the message requests access
4 to services, such that nodes receiving the message in other ones of the security domains can
5 bypass authentication of the party for access to services of that other security domain, upon
6 verifying authenticity of the authentication authority and establishing that the authentication
7 authority vouches for the received message.

1 14. The method according to Claim 13, wherein the authentication authority is determined to
2 vouch for the received message if a digital signature computed by the authentication authority and
3 transmitted with the message is determined, by the node receiving the message in the one of the
4 other security domains, to be valid.

1 15. The method according to Claim 13, wherein the transmitted message contains security
2 credentials of the party, where those security credentials have been authenticated by the identified
3 authentication authority and are protected such that only authorized ones of the nodes receiving
4 the message in other ones of the security domains can access the protected security credentials.

1 16. The method according to Claim 15, wherein the protected security credentials are
2 encrypted using a public key of each of the authorized ones of the nodes receiving the message,
3 such that each of the authorized ones can decrypt the protected security credentials using a
4 corresponding private key.

1 17. A system for achieving context-sensitive confidentiality among security domains within a
2 federated environment, the system comprising:

3 means for determining a route to be taken by a message to be transmitted in the federated
4 environment, where the route spans a plurality of the security domains;

5 means for determining rights of nodes to be encountered on the determined route to
6 access security-sensitive portions of the message;

7 means for selectively protecting the security-sensitive portions of the message, according
8 to the determined access rights; and

9 means for transmitting the message with its selectively-protected portions on the
10 determined route.

1 18. A computer program product for securely transmitting context-sensitive confidential

2 message content among security domains within a federated environment, the computer program
3 product embodied on one or more computer-readable media and comprising:

4 computer-readable program code means for determining a route to be taken by a message
5 to be transmitted in the federated environment, where the route spans a plurality of the security
6 domains;

7 computer-readable program code means for determining rights of nodes to be encountered
8 on the determined route to access security-sensitive portions of the message;

9 computer-readable program code means for selectively protecting the security-sensitive
10 portions of the message, according to the determined access rights; and

11 computer-readable program code means for transmitting the message with its selectively-
12 protected portions on the determined route.

1 19. A method of providing a message confidentiality service for securely transmitting
2 messages among security domains within a federated environment, the method comprising steps
3 of:

4 determining a route to be taken by a message to be transmitted in the federated
5 environment, where the route spans a plurality of the security domains;

6 determining rights of nodes to be encountered on the determined route to access security-
7 sensitive portions of the message; and

8 determining how the security-sensitive portions of the message should be protected,
9 according to the determined access rights.

1 20. The method according to Claim 20, further comprising the step of charging a fee for one
2 or more of the determining steps.

1 21. The method according to Claim 20, further comprising the step of applying the determined
2 protections to the security-sensitive portions.